PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-164549

(43)Date of publication of application : 19.06.1998

(51)Int.Cl. H04N 7/167
H04N 5/225
H04N 7/18

(21)Application number : 08-317526

(22)Date of filing : 28.11.1996

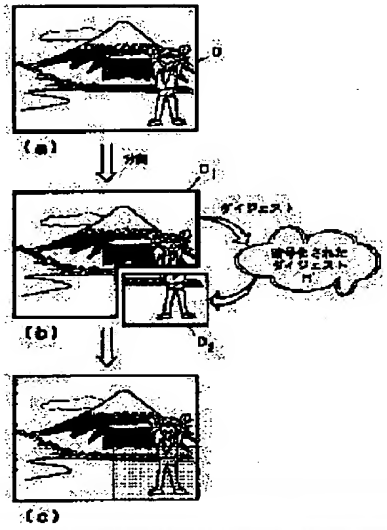
(71)Applicant : IBM JAPAN LTD

(72)Inventor : SHIMIZU SHUICHI
NUMAO MASAYUKI
MORIMOTO NORISHIGE

(54) SYSTEM FOR HIDING IN AUTHENTICATION INFORMATION IS IMAGE AND IMAGE AUTHENTICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a new system capable of supplying authentication information in a form which is inseparable from an image data. SOLUTION: An image is halved and authentication information to hide in one image is obtained from the other image itself. Objective image data photographed by a digital camera is divided into an area D1 for generating a hush value and an area D2 for hiding a hush value H. A digest-calculating part calculates H from data of D1 and ciphers it by a secret key different for each digital camera, etc., to hide D2, hiding can be executed by operating a pixel value in a real space or a frequency space to a degree of not being recognized visually. In D2, additional information such as a time stamp, positional information of GPS can be hidden before hiding data from D1.



LEGAL STATUS

[Date of request for examination] 27.08.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3154325

[Date of registration] 02.02.2001

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] By operating the data in a field division means to divide an image into the 1st image field and the 2nd image field, an authentication information generation means to generate authentication information from the data in said 1st image field, and said 2nd image field The system which hides into an image the authentication information characterized by having a field composition means to compound a hiding means to hide said authentication information all over said 2nd image field, and said 1st image field in said image and said 2nd image field in which said authentication information was hidden.
[Claim 2] Said authentication information is a system according to claim 1 characterized by being the digest of the data in said 1st image field.
[Claim 3] Said digest is a system according to claim 2 characterized by being the hash value of the data in said 1st image field.
[Claim 4] It is the system according to claim 1 which has further a code conversion means to encipher said authentication information, and is characterized by said hiding means hiding the enciphered authentication information concerned all over said 2nd image field.
[Claim 5] A field specification means to pinpoint in an image the 1st image field and the 2nd image field in which information was hidden by operating data, An authentication information generation means to generate the 1st authentication information from the data in said 1st image field, The image authentication system characterized by having an extract means to extract the 2nd authentication information from said 2nd image field, and an authentication means to judge that said image is not changed when said 1st authentication information is in agreement with said 2nd authentication information.
[Claim 6] Said authentication means is a system according to claim 6 characterized by judging that said image is changed when said 1st authentication information is not in agreement with said 2nd authentication information.
[Claim 7] Said 1st authentication information is a system according to claim 5 characterized by being the digest of the data in said 1st image field.
[Claim 8] Said digest is a system according to claim 6 characterized by being the hash value of the data in said 1st image field.
[Claim 9] It is the system according to claim 5 characterized by judging that said image is not changed when said 2nd authentication information is enciphered, and it has further a decode conversion means to decrypt said 2nd authentication information and the decrypted authentication information of said authentication means concerned corresponds with said 1st authentication information.
[Claim 10] By operating the data in the step which divides an image into the 1st image field and the 2nd image field, the step which generates authentication information from the data in said 1st image field, and said 2nd image field How to hide into an image the authentication information characterized by having the step which compounds the step which hides said authentication information all over said 2nd image field, and said 1st image field in said image and said 2nd image field in which said authentication information was hidden.
[Claim 11] The step which pinpoints in an image the 1st image field and the 2nd image field in which

information was hidden by operating data, The step which generates the 1st authentication information from the data in said 1st image field, It is the authentication approach about the identity of the image characterized by having the step which extracts the 2nd authentication information from said 2nd image field, and the step judged that said image is not changed when said 1st authentication information is in agreement with said 2nd authentication information.
[Claim 12] By changing into an electrical signal the light inputted through optical system and said optical system The transducer which outputs the analog signal of an image, and a signal-processing means to generate the digital signal of an image according to said analog signal, A field division means to divide an image into the 1st image field and the 2nd image field according to said digital signal, By operating the data in an authentication information generation means to generate authentication information from the data in said 1st image field, a code conversion means to encipher said authentication information, and said 2nd image field The digital camera characterized by having a field composition means to compound a hiding means to hide the enciphered authentication information all over said 2nd image field, and said 1st image field in said image and said 2nd image field in which said authentication information was hidden.
[Claim 13] Said authentication information is a digital camera according to claim 12 characterized by being the hash value of the data in said 1st image field.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The field of the invention to which invention belongs] This invention relates to the system which hides the digest of an image, and relates to the digital camera which adds the authentication information on the image photoed especially to this image.
[0002]
[Description of the Prior Art] Recently, a digital camera is spreading quickly. A digital camera photos a scene etc. and saves it by making this into digital data at memory card etc. The reason of rapid spread of a digital camera has a more important thing in the point that the taken photograph can be saved as a digital image, although it is naturally in the fall of a body price, or its outstanding portability. By computer, according to liking of a user, the contents are processed easily, and digital data can carry out the thing of them, and can be easily circulated through a network etc. Therefore, it is expected that the need for a digital camera that such a digital image can be obtained easily becomes larger future still.
[0003] On the other hand, since digital data is easy to alter composition etc. so that a trace may not remain, the dependability as a proof of the photoed digital image may pose a problem. Such a problem can pose a big problem in the photography in business, although it will seldom be generated if it is hobby photography extent by the general user. For example, it is the case where the digital image photoed

between the contract points through the network in using a digital camera as construction record of an construction work **** the ordering agency is transmitted and received. The digital image photoed in these cases can demonstrate the function as documentary photography only after it can attest the identity of the contents. Therefore, the expectation for the digital camera which can add the authentication information about the identity of the photoed digital image is great.

[0004] Drawing 1 is the block diagram of the image-processing system of the conventional digital camera. The photoed object is changed into an electric analog signal by CCD12 through optical system 11. This signal is processed by the signal-processing section 13, and is outputted as image data D which is a digital signal. This generated image data D is inputted into the digest count section 14. The digest count section 14 calculates hash value H of the data of the whole image. A hash value is a value (digest) which becomes settled in the meaning which shows the description of an image by the operation based on image data. Hash value H as a digest will become a different value if the contents of an image differ. The code transducer 15 enciphers hash value H using a private key SK, and outputs enciphered hash value H'. This enciphered hash value H' is authentication information, and this is attached in the form of another file with image data D.

[0005] The following information is required in order for image data to judge whether it is the same as that of original image data, or image data is not altered, if it puts in another way.

(1) Image data (2) authentication information (it attaches to image data as another file)

(3) The public key PK corresponding to a private key SK (it receives separately from those who have authority)

[0006] Those who detect an alteration calculate the hash value H1 of the image data which it is going to attest first. Next, a hash value H2 is specified from the authentication information in an attached file. Since it is what enciphered hash value H of the subject-copy image D with the private key SK (hash value H'), if this authentication information remains as it is, it cannot specify a hash value H2. Then, from the authority **** person who is keeping the public key PK corresponding to a private key SK, this public key PK comes to hand, and authentication information is decrypted based on this. And the obtained hash value H2 is compared with the calculated hash value H1. Both value must be in agreement if the image as a candidate for authentication is the same as the subject-copy image D. The hash value as a digest is because the values should differ if the contents of the image differ. Therefore, when a hash value is in agreement, identity is attested, and in differing, it judges it as what was altered.

[0007]

[Problem(s) to be Solved by the Invention] Thus, it attests on the assumption that, as for image data, authentication of the identity in a Prior art attaches authentication information independently and authentication information is attached at the time of verification. Therefore, when authentication information is missing, it cannot verify any longer. Therefore, the verification person had to pay careful attention to storage and management of authentication information.

[0008] Then, the purpose of this invention is proposing the new method which can supply authentication information in a format really indivisible from image data.

[0009] Moreover, another purpose of this invention is to enable verification of image data, without a verification person keeping authentication information.

[0010] Furthermore, another purpose of this invention is hiding authentication information into an image, without degrading the image quality of image data.

[0011]

[Means for Solving the Problem] A field division means by which the 1st invention divides an image into the 1st image field and the 2nd image field in order to solve the above-mentioned technical problem, By operating the data in an authentication information generation means to generate authentication information from the data of the 1st image field, and the 2nd image field The system which hides the authentication information which has a field composition means to compound a hiding means to hide authentication information all over the 2nd image field, and the 1st image field in an image and the 2nd

image field in which authentication information was hidden in a way stage of an image is offered.
[0012] A field specification means by which the 2nd invention pinpoints in an image the 1st image field and the 2nd image field in which information was hidden by operating data, An authentication information generation means to generate the 1st authentication information from the data in the 1st image field, It judges that the image is not changed when an extract means to extract the 2nd authentication information, and the 1st authentication information are in agreement with the 2nd authentication information from the 2nd image field, and in not being in agreement, it offers the image authentication system which has an authentication means to judge that the image is changed.
[0013] The 3rd invention by operating the data in the step which divides an image into the 1st image field and the 2nd image field, the step which generates authentication information from the data in the 1st image field, and the 2nd image field The approach of hiding the authentication information which has the step which compounds the step which hides authentication information all over the 2nd image field, and the 1st image field in an image and the 2nd image field in which authentication information was hidden in a way stage of an image is offered.
[0014] The step at which the 4th invention pinpoints in an image the 1st image field and the 2nd image field in which information was hidden by operating data, The step which generates the 1st authentication information from the data in the 1st image field, The authentication approach is offered for the identity of the image which has the step which extracts the 2nd authentication information from the 2nd image field, and the step judged that the image is not changed when the 1st authentication information is in agreement with the 2nd authentication information.
[0015]
[Function] With such a configuration, authentication information (the 2nd) is hidden all over the 2nd image field. (The 2nd) Authentication information is the information for attesting the identity of an image, and is a peculiar thing which changes with contents of the 1st image field. The 1st authentication information generated based on the changed data when the data in the 1st image field are changed serves as a value which hides all over the 2nd image field and is different from the authentication information on ********** 2nd. Therefore, the 2nd authentication information hidden all over the 2nd image field is extracted, and it is verifiable whether the image is changed or not, if it compares with the 1st authentication information which newly generated it from the 1st image field.
[0016]
[Embodiment of the Invention]
[Digital camera] drawing 2 is the block diagram of the image-processing system of the digital camera in this example. The photoed object is changed into an electric analog signal by CCD22 through optical system 21. This signal is processed by the image-processing section 27 which has the signal-processing section 23, the field division section 24, the hiding section 25, and the field composition section 26, is outputted as image data D' which is a digital signal, and is saved in the storage sections 28, such as memory card. Although this image data D' is not the completely same data as image data D since a hash value is hidden in the predetermined image field in image data D by the hiding section 25, it cannot recognize that difference visually.
[0017] Image data D which is the output of the signal-processing section 23 can be carved into two fields by the field division section 24. Drawing 3 is a conceptual diagram for explaining division and composition of an image field. The image D as shown in this drawing (a) is divided into the image field D1 which gives the input value for hash value generation, and the image field D2 which embeds generated hash value H (refer to this drawing (b)). In this example, it is possible for the image field D2 to consist of 40x40 pixels at the lower right of an image, and to hide 160-bit information ideally.
[0018] The image field D1 divided by the field division section 23 is inputted into the digest count section 29 as the authentication information generation section. The digest count section 29 calculates hash value H of the data of the image field D1 cut-off whole as authentication information. A hash value is a digest in which the description of an image is shown by the operation based on image data. A digest

is an epitome which shows the description of image data, and hash value H as a digest reacts sensitively also to 1-pixel modification of the contents of an image, and has the property to change to a completely different value. Therefore, it is possible that it is the numeric value which has natural image data and the relation of about 1 to 1 especially.

[0019] Hash value H is specifically expressed by the following formulas.

[Equation 1]

H=H1 (d[0]//d[1]//d [2] //... //d [I])

[0020] Here, H1 is a Hash Function. Moreover, a operator "//" means that each element of a message array is connected. Moreover, d [i] shows each pixel value included all over the image field D1. The exclusive OR of the data which an array element has is sufficient as this concrete operation. However, when it considers as an exclusive OR, the sequence of a message array value is not reflected in a count result. For example, if the approach of CRC (Cyclic Redundancy Check) is used, this order relation can be reflected. This algorithm is one of the algorithms for calculating a checksum, and generates the output for which it depended in order of the contents of the data stream, and a data stream.

[0021] This Hash Function H1 is a function with which cutting tool length asks for the output (hash value) of different cutting tool length K from it from the input (array value d [i]) which is Bm cutting tool. Since this function is a one-way function, it cannot presume x as a matter of fact from y in H(x) =y. A hash value is only used as initial value in the case of data hiding, and a different output to a different input should just carry out it being guaranteed as a matter of fact. Therefore, there is no special semantics in the value of a hash value itself. An important thing is that a hash value becomes settled uniquely based on the contents of whole outputting the value which shows the description of an array by the operation, i.e., an array element, and the value changes with contents of the whole array.

[0022] The code transducer 30 enciphers hash value H using a private key SK, and outputs enciphered hash value H'. This enciphered hash value H' is authentication information. A private key SK is [0023] currently held inside the camera using a different key for every digital camera. Hash value H' enciphered as authentication information is sent to the hiding section 25 in the image-processing section 27. The hiding section 25 hides hash value H' all over the image field D2 by operating the data in [D2] an image field. A hide lump can be carried out in real space or frequency space by operating the data in the image field D2 (for example, pixel value). Although embedding can consider various approaches, it mentions later about the example. In addition, this is explained to Japanese Patent Application No. No. (we reference number JA 996-044) 159330 [eight to], and Japanese Patent Application No. No. (we reference number JA 996-074) 272721 [eight to] at the detail.

[0024] Since the data in the field are operated in order to hide hash value H' all over the image field D2, the image quality in the part is somewhat different from the subject-copy image. However, since most things for which such a difference is recognized visually are the impossible, visual degradation of image quality is not produced.

[0025] The field composition section 26 compounds the image field D1 in a subject-copy image, and the image field D2 in which hash value H' was hidden (refer to drawing 3 (c)). And this compounded image data D' is saved in the storage section 28.

[0026] Since the field which is not related to count of a digest and to embed is pinpointed, division of an image field is performed so that clearly from the above-mentioned explanation. Supposing it calculates the digest of the whole image and hides that result, without dividing an image field, it stops being in agreement with the original digest of this with which the new digest of the whole image after a lump is embedded by hiding. Therefore, identity of an image cannot be attested by such approach. Then, the image field in which a digest is hidden has guaranteed coincidence with the calculated digest and the digest hidden by not considering as the object of digest count. In such a viewpoint, it is good also considering the subject-copy image D which smeared away only the part of the image field D2 in monochrome, such as black and white, as an image field D1. In this case, the digest of the subject-copy image D with which the part was smeared away is calculated, and it is hidden in the image field D2.

Thereby, it can hide and coincidence of a digest can be guaranteed after a lump.
[0027] In addition, the digital camera in this example may hide the additional information of the positional information measured by time stamps, such as ID of a photography camera, and a date of photography, and GPS all over the image field D1. In this case, it is important to hide additional information all over the image field D1, to be ****** and to hide hash value H' of that result in the image field D2 after that first. It is because a hash value is different, so authentication of identity becomes impossible by hide it of subsequent additional information when hash value H' of the image before embedding additional information is hidden in the image field D2.
[0028] In addition, it is not necessary to concentrate on one place like the above-mentioned example, and the image field D2 may be dispersedly made to exist using a location sequence generation algorithm, and a part of Low Bit may be used for it.
[0029] The system which performs identity authentication of the image photoed with the digital camera is explained using a [image authentication system], next the hidden authentication information. Those who are going to verify identity need to have the following information. Since authentication information is hidden in the really indivisible condition into an image, please care about the point which does not need to be kept in the form of another file.
(1) The public key PK corresponding to the image data M'(2) private key SK (it receives separately from those who have authority)
[0030] Drawing 4 is the block diagram of the identity authentication system of the image in this example. The field specification section 41 pinpoints the image field D1 and the image field D2 in image D' in which hash value H' is hidden. The image field D1 is a field which gives the data for generating a hash value, and the image field D2 is a field in which hash value H' as above-mentioned authentication information is hidden.
[0031] The digest count section 42 newly calculates a hash value based on the data in the image field D1. Moreover, the digest extract section 43 extracts enciphered hash value H' which is hidden as authentication information from the image field D2. The concrete extract approach is later mentioned with the concrete approach of embedding.
[0032] The decode transducer 44 decodes extracted hash value H' using a public key PK. This public key PK is an available key which becomes settled uniquely corresponding to a private key SK, and needs to come to hand from the authority **** person who is keeping this.
[0033] In the authentication section 45, identity is attested by comparing the hash value based on the data in the image field D1 newly calculated by the digest count section 42 with hash value H' obtained by the decode transducer 44. That is, when a hash value is in agreement, it is judged that the image is not altered. Moreover, when a hash value is not in agreement, it is judged that the image is altered. That the case where a hash value is not in agreement arises is the case where it corresponds to at least the following two one side.
(1) Since the hash value which newly re-**(ed) from the image field D1 changes when the image field D1 is altered, stop being in agreement with hash value H hidden all over the image field D2.
(2) Since hash value H hidden in the image field D2 changes when the image field D2 is altered, stop being in agreement with the hash value which re-**(ed) from the image field D1.
[0034] Since according to this example authentication information unifies in an image and is hidden by using a data hiding technique, it is not necessary to attach authentication information to image data as another file. Therefore, it is verifiable even if the verification person does not hold especially authentication information.
[0035] Moreover, since authentication information is enciphered using the public key cryptosystem (scramble), rewriting of the authentication information by the holder in bad faith can be made impossible as a matter of fact. Furthermore, a certain public key PK is equivalent to only one private key SK. Therefore, the digital image of a private key SK is possible also for attesting with which digital camera a photograph was taken by making it different for every digital camera.

[0036] In addition, in order to open a digital camera and to oppose unjust access to the maintenance information inside a body, it is effective to use devices, such as a tamper-proof module used with the cellular phone etc. It is regarded as that to which the theft of the private key SK was carried out when such unlawful access was performed, and about the image data based on the private key SK, even when a digest is in agreement, a thing judging is altered and carried out. By doing in this way, the damage by a third person's unjust action is avoidable.
[0037] In addition, although the above-mentioned example explained the digital camera, as for this invention, it is natural that it is not limited to this and can use for digital systems, such as a digital video, widely.
[0038]
[Example] Here, pixel block coding (Pixel Block Coding) (henceforth PBC) which is an example of an approach which extracts the approach of embedding the data set as the object of a concealment into a certain media data of a certain and the data embedded conversely is explained. When PBC is used, hiding and an extract are processed according to a certain following transformation rules which are expressed in data.
[0039] [Basic algorithm] Generally primary properties, such as a pixel value of two pixels which adjoined, have the high correlation mutually. Therefore, even if it puts in and changes a pixel value, an image does not produce degradation of extent which can be recognized visually. In view of this property, this algorithm defines the image field which has at least one pixel as a pixel block, is replacing the characteristic value of the pixel block which adjoined intentionally based on a certain transformation rule, and conceals 1-bit data. That is, data are expressed by exchange of the characteristic value of an adjoining pixel block. Moreover, at the time of the extract of data, data are extracted according to the extract regulation determined based on these transformation rule.
[0040] Bit information replaces the characteristic value (for example, brightness value) of two adjoining pixel blocks according to the following transformation rules, and a thing expression is carried out.
[0041] bit-on <1> : case the characteristic value of one pixel block (PB1) is larger than the characteristic value of another side (PB2) -- bit - off <0> : [case the characteristic value of one pixel block (PB1) is smaller than the characteristic value of another side (PB2) -- 0042] Moreover, bit information is extracted by comparing the characteristic value (for example, brightness value) of two adjoining pixel blocks according to the following extract regulations.
[0043] case the characteristic value of one pixel block (PB1) is larger than the characteristic value of another side (PB2) -- :bit-on case the characteristic value of <1> one pixel block (PB1) is smaller than the characteristic value of another side (PB2) -- :bit - off <0 [0044]> Drawing 5 is drawing for explaining hiding of data and the extract which used PBC. It is also possible to define the pixel blocks PB1 and PB2 as a set of two or more pixels like 3x3 pixels, and to define 1 pixel as a 1-pixel block. Since the adjoining pixel block has high correlation, even if it replaces those locations, it is not sensed that the image deteriorated in extent which can be recognized visually (drawing 5 (a)).
[0045] The case where the location of the pixel block in an original image is this drawing (b) is considered. First, the characteristic value of two pixel blocks is compared, consequently the direction of the characteristic value of PB1 presupposes that it is larger than the characteristic value of PB2. Since the conditions of data "data [in / when concealing 1" / in the characteristic value of a pixel block / transformation rule]" 1" are already fulfilled originally, there is no exchange line crack of the characteristic value of these blocks. Since the extract regulation has determined that it is data "1" when the characteristic value of PB1 is large in case data are extracted, data"1" is extracted.
[0046] on the other hand -- original -- data -- " -- zero -- " -- concealing -- a case -- original -- it can set -- a pixel - a block -- a characteristic value -- relation -- transformation rule -- it can set -- data -- " -- zero -- " -- conditions -- not filling -- since -- the characteristic value of a pixel block - - changing . However, this exchange cannot be recognized visually. At the time of an extract, data"0" is extracted from the relation of the characteristic value of these blocks according to an extract regulation.

[0047] Thus, a number sufficient in PBC to conceal the information set as the object of a concealment of pixel blocks are chosen from images. And the train of this pair is generated by making the pair of the pixel block which adjoins a pixel block and it of selected 1. And the bit which serves as a candidate for a concealment one by one from the head of a train is concealed.
[0048] This train may be matched with the condition sequence S in the 1st example. For example, a pixel block is matched with the array element M of the media array M in the 1st example. A pair is made from the media array value which adjoins each array element (status value Sj) of a condition sequence and it which were serially generated by the target in the hiding activity. And, of course, it is also possible to determine again based on the pseudo-random number sequence it is [a pseudo-random number sequence] possible to perform the above-mentioned processing to this pair and which is generated from the kind (seed) of a certain random number.
[0049] At the time of an extract, the same block train as the time of hiding is scanned. The whole message is extracted by collecting [1-bit] at a time whether each pair expresses bit-on or OFF is expressed according to an extract regulation. Supposing the characteristic value of the pixel block which is a pair is the same, the pair will be skipped like the time of hiding. If a block train or its train generation method is made secret, the concealed information can be hidden from others.
[0050] In addition, as for an embedding location, in PBC, it is desirable to determine in view of image quality and extract precision. That is, when the difference of the characteristic value of the pixel block which constitutes the pair used as an embedding object is not much large, there is a possibility that image quality may deteriorate by exchange actuation. In order to control degradation of such image quality, it is desirable to establish the 1st threshold (upper limit), and to make it not embed a bit in the pair, if the difference of a characteristic value is beyond the threshold.
[0051] Moreover, although degradation of the image quality by exchange actuation will hardly be produced if the difference of a characteristic value is small, size relation is conversely reversed under the effect of a noise, and there is a possibility that the bit embedded at the time of an extract cannot be extracted. Therefore, in order to control the fall of extract precision, it is desirable to establish the 2nd threshold (minimum), and to make it not embed a bit in the pair, if the difference of a characteristic value is below the threshold.
[0052] It skips without operating anything in the pair applicable to these cases. And the bit information which should be concealed is postponed and it conceals for the following pair.
[0053] As a [characteristic value of block] characteristic value, things can be carried out using the value about the primary property of a pixel block, and the value about a secondary property. A primary property is the direct parameter of a pixel value like the brightness of a pixel block, or a chromaticity. Moreover, a secondary property is acquired by decomposing primary ****** like the value which shows the average of said parameter, and the statistical property of distribution. Furthermore, a characteristic value is good also as the result of an operation of the array which consists of two or more pixel values, and a predetermined array (mask), and can also be considered as the specific element value obtained by performing frequency conversion. Generally, the primary property has the high correlation in two adjoining pixel blocks. On the other hand, a secondary property may have a high correlation in two blocks not adjoining and which separated. Therefore, the pixel block set as the object of pBC should care about the point which is not limited to the block which not necessarily adjoins.
[0054]
[Effect] Thus, since authentication information is supplied in a format really indivisible from image data, i.e., the format hidden into the image, according to this invention, a verification person does not independently need to keep authentication information. Even if it performs a hide lump of such authentication information, image quality of image data is not degraded.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram of the image-processing system of the conventional digital camera.
[Drawing 2] It is the block diagram of the image-processing system of the digital camera in this example.
[Drawing 3] It is the block diagram of the identity authentication system of the image in this example.
[Drawing 4] It is the block diagram of the identity authentication system of the image in this example.
[Drawing 5] It is drawing for explaining hiding of the data using PBC, and an extract.
[Description of Notations]
21 ... Optical system
22 ... CCD
23 ... Signal-processing section
24 ... Field division section
25 ... Hiding section
26 ... Field composition section
27 ... Image-processing section
28 ... Storage section
29 ... Digest count section
30 ... Code transducer

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－164549

(43)公開日　平成10年(1998)６月19日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｎ	7/167	Ｈ０４Ｎ	7/167	Ｚ
	5/225		5/225	Ｚ
	7/18		7/18	Ｖ

審査請求　未請求　請求項の数13　ＯＬ　（全 10 頁）

(21)出願番号　特願平8－317526

(22)出願日　平成８年(1996)11月28日

(71)出願人　592073101
日本アイ・ビー・エム株式会社
東京都港区六本木３丁目２番12号

(72)発明者　清水　周一
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社東京基礎研究所内

(72)発明者　沼尾　雅之
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社東京基礎研究所内

(72)発明者　森本　典繁
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社東京基礎研究所内

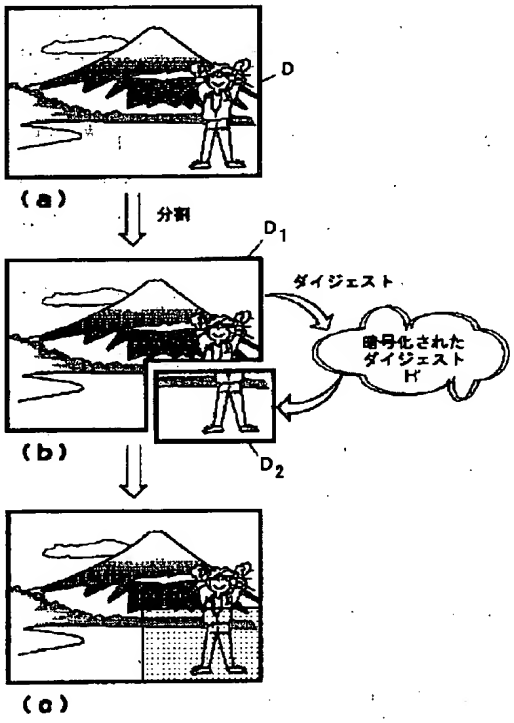
(74)代理人　弁理士　合田　潔　（外２名）

(54)【発明の名称】　認証情報を画像に隠し込むシステム及び画像認証システム

(57)【要約】　（修正有）

【課題】従来の画像へのデータハイディングでは検証するまで認証情報を添付しておく必要があり、それが欠落していると検証ができなかった。

【解決手段】画像を２つに分割し、一方の画像に隠し込む認証情報を他方の画像そのものから得るようにする。デジタル・カメラにおいて撮影された対象の画像データは、ハッシュ値を生成するための領域ＤＩと生成されたハッシュ値Ｈを隠し込む領域Ｄ２とに分割される。ダイジェスト計算部はＤ１のデータからＨを計算し、デジタル・カメラごとに異なる秘密鍵で暗号化するなどして、Ｄ２に隠し込む。隠し込みは視覚的に認識できない程度に実空間や周波数空間で画素値を操作することにより行うことができる。Ｄ２には、Ｄ１からのデータの隠し込みの前に、タイム・スタンプやＧＰＳの位置情報といった付加情報を隠し込んでおくこともできる。



1

【特許請求の範囲】

【請求項１】第１の画像領域と，第２の画像領域とに画像を分割する領域分割手段と，前記第１の画像領域中のデータから認証情報を生成する認証情報生成手段と，前記第２の画像領域中のデータを操作することにより，前記認証情報を前記第２の画像領域中に隠し込むハイディング手段と，前記画像における前記第１の画像領域と前記認証情報が隠し込まれた前記第２の画像領域とを合成する領域合成手段とを有することを特徴とする認証情報を画像中に隠し込むシステム。

【請求項２】前記認証情報は，前記第１の画像領域中のデータのダイジェストであることを特徴とする請求項１に記載のシステム。

【請求項３】前記ダイジェストは，前記第１の画像領域中のデータのハッシュ値であることを特徴とする請求項２に記載のシステム。

【請求項４】前記認証情報を暗号化する暗号変換手段をさらに有し，前記ハイディング手段は当該暗号化された認証情報を前記第２の画像領域中に隠し込むことを特徴とする請求項１に記載のシステム。

【請求項５】第１の画像領域と，データを操作することにより情報が隠し込まれた第２の画像領域とを画像中において特定する領域特定手段と，前記第１の画像領域中のデータから第１の認証情報を生成する認証情報生成手段と，前記第２の画像領域から，第２の認証情報を抽出する抽出手段と，前記第１の認証情報が前記第２の認証情報と一致する場合に，前記画像が改変されていないと判断する認証手段とを有することを特徴とする画像認証システム。

【請求項６】前記認証手段は，前記第１の認証情報が前記第２の認証情報と一致しない場合には，前記画像が改変されていると判断することを特徴とする請求項６に記載のシステム。

【請求項７】前記第１の認証情報は，前記第１の画像領域中のデータのダイジェストであることを特徴とする請求項５に記載のシステム。

【請求項８】前記ダイジェストは，前記第１の画像領域中のデータのハッシュ値であることを特徴とする請求項６に記載のシステム。

【請求項９】前記第２の認証情報は暗号化されており，前記第２の認証情報を復号化する復号変換手段をさらに有し，かつ，前記認証手段は，当該復号化された認証情報が前記第１の認証情報と一致する場合に，前記画像が改変されていないと判断することを特徴とする請求項５に記載のシステム。

【請求項１０】第１の画像領域と，第２の画像領域とに画像を分割するステップと，前記第１の画像領域中のデータから認証情報を生成するステップと，前記第２の画像領域中のデータを操作することにより，前記認証情報を前記第２の画像領域中に隠し込むステップと，前記画

2

像における前記第１の画像領域と前記認証情報が隠し込まれた前記第２の画像領域とを合成するステップとを有することを特徴とする認証情報を画像中に隠し込む方法。

【請求項１１】第１の画像領域と，データを操作することにより情報が隠し込まれた第２の画像領域とを画像中において特定するステップと，前記第１の画像領域中のデータから第１の認証情報を生成するステップと，前記第２の画像領域から，第２の認証情報を抽出するステップと，前記第１の認証情報が前記第２の認証情報と一致する場合に，前記画像が改変されていないと判断するステップとを有することを特徴とする画像の同一性を認証方法。

【請求項１２】光学系と，前記光学系を介して入力された光を電気信号に変換することにより，画像のアナログ信号を出力する変換器と，前記アナログ信号に応じて，画像のデジタル信号を生成する信号処理手段と，前記デジタル信号に応じて，画像を，第１の画像領域と，第２の画像領域とに分割する領域分割手段と，前記第１の画像領域中のデータから認証情報を生成する認証情報生成手段と，前記認証情報を暗号化する暗号変換手段と，前記第２の画像領域中のデータを操作することにより，暗号化された認証情報を前記第２の画像領域中に隠し込むハイディング手段と，前記画像における前記第１の画像領域と前記認証情報が隠し込まれた前記第２の画像領域とを合成する領域合成手段とを有することを特徴とするデジタル・カメラ。

【請求項１３】前記認証情報は，前記第１の画像領域中のデータのハッシュ値であることを特徴とする請求項１２に記載のデジタル・カメラ。

【発明の詳細な説明】

【０００１】

【発明の属する利用分野】本発明は，画像のダイジェストを隠し込むシステムに係り，特に，撮影された画像の認証情報をこの画像に付加するデジタル・カメラに関する。

【０００２】

【従来の技術】最近，デジタル・カメラが急速に普及しつつある。デジタル・カメラは，景色などを撮影し，これをデジタル・データとしてメモリー・カードなどに保存するものである。デジタル・カメラの急速な普及の理由は，本体価格の低下やその優れた携帯性にあることは当然であるが，より重要なことは，撮影された写真をデジタル画像として保存できる点にある。デジタル・データは，コンピュータにより，ユーザの好みに応じて内容を容易に加工することでき，かつネットワークなどを介して容易に流通させることができる。従って，このようなデジタル画像を簡単に得ることができるデジタル・カメラの必要性は，今後ますます大きくなるものと期待されている。

【０００３】その一方で，デジタル・データは，痕跡が残らないように合成などの改ざんを行うことが容易であるため，撮影されたデジタル画像の証拠としての信頼性が問題となる場合がある。このような問題は，一般ユーザによる趣味的な撮影程度であればあまり生じないであろうが，ビジネスにおける撮影では大きな問題となり得る。例えば，建設工事の工事記録としてデジタル・カメラを用いたり，発注元と請負先との間で，ネットワークを通じて，撮影されたデジタル画像を送受信する場合である。これらの場合，撮影されたデジタル画像は，その内容の同一性を認証できて，初めて証拠写真としての機能を発揮することができる。従って，撮影されたデジタル画像の同一性に関する認証情報を付加できるデジタル・カメラへの期待は大きい。

【０００４】図１は，従来のデジタル・カメラの画像処理系のブロック図である。撮影された対象は，光学系１１を介して，ＣＣＤ１２により電気的なアナログ信号に変換される。この信号は信号処理部１３により処理され，デジタル信号である画像データＤとして出力される。この生成された画像データＤは，ダイジェスト計算部１４に入力される。ダイジェスト計算部１４は，画像全体のデータのハッシュ値Ｈを計算する。ハッシュ値は，画像データに基づいた演算により画像の特徴を示す一意に定まる値（ダイジェスト）である。ダイジェストとしてのハッシュ値Ｈは，画像内容が異なれば，相違する値となる。暗号変換部１５は，ハッシュ値Ｈを秘密鍵ＳＫを用いて暗号化し，暗号化されたハッシュ値Ｈ’を出力する。この暗号化されたハッシュ値Ｈ’が認証情報であり，これは画像データＤとは別ファイルの形で添付される。

【０００５】画像データがオリジナルの画像データと同一であるか，換言すると，画像データが改ざんされていないかを判断するためには，以下の情報が必要である。

（１）画像データ

（２）認証情報（別ファイルとして画像データに添付）

（３）秘密鍵ＳＫに対応した公開鍵ＰＫ（権限を有する者から別途入手）

【０００６】改ざんを検出する者は，まず認証しようとする画像データのハッシュ値H_1を計算する。次に添付ファイル中の認証情報からハッシュ値H_2を特定する。この認証情報は，原画像Ｄのハッシュ値Ｈを秘密鍵ＳＫにより暗号化したもの（ハッシュ値Ｈ’）なので，そのままではハッシュ値H_2を特定することはできない。そこで，秘密鍵ＳＫに対応した公開鍵ＰＫを保管している権限ある者から，この公開鍵ＰＫを入手し，これに基づいて，認証情報を復号化する。そして，得られたハッシュ値H_2を，計算したハッシュ値H_1と比較する。認証対象としての画像が原画像Ｄと同一であれば，両者の値は一致するはずである。ダイジェストとしてのハッシュ値は，画像の内容が異なれば，その値が異なっているはずだからである。従って，ハッシュ値が一致する場合には，同一性を認証し，異なる場合には，改ざんされたものと判断する。

【０００７】

【発明が解決しようとする課題】このように，従来の技術における同一性の認証は，画像データとは別に認証情報を添付し，検証時に認証情報が添付されていることを前提に認証を行うものである。従って，認証情報が欠落している場合にはもはや検証を行うことができない。従って，検証者は，認証情報の保管・管理に細心の注意を払わねばならなかった。

【０００８】そこで，本発明の目的は，認証情報を画像データと一体不可分な形式で供給することが可能な新規な方式を提案することである。

【０００９】また，本発明の別の目的は，検証者が認証情報を保管することなく，画像データの検証を可能にすることである。

【００１０】さらに，本発明の別の目的は，画像データの画質を劣化させることなく，画像中に認証情報を隠し込むことである。

【００１１】

【課題を解決するための手段】上記課題を解決するために，第１の発明は，画像を第１の画像領域及び第２の画像領域に分割する領域分割手段と，第１の画像領域のデータから認証情報を生成する認証情報生成手段と，第２の画像領域中のデータを操作することにより，認証情報を第２の画像領域中に隠し込むハイディング手段と，画像における第１の画像領域と認証情報が隠し込まれた第２の画像領域とを合成する領域合成手段とを有する認証情報を画像の一手段に隠し込むシステムを提供する。

【００１２】第２の発明は，第１の画像領域と，データを操作することにより情報が隠し込まれた第２の画像領域とを画像中において特定する領域特定手段と，第１の画像領域中のデータから第１の認証情報を生成する認証情報生成手段と，第２の画像領域から，第２の認証情報を抽出する抽出手段と，第１の認証情報が第２の認証情報と一致する場合に，画像が改変されていないと判断し，一致しない場合には，画像が改変されていると判断する認証手段とを有する画像認証システムを提供する。

【００１３】第３の発明は，第１の画像領域と，第２の画像領域とに画像を分割するステップと，第１の画像領域中のデータから認証情報を生成するステップと，第２の画像領域中のデータを操作することにより，認証情報を第２の画像領域中に隠し込むステップと，画像における第１の画像領域と認証情報が隠し込まれた第２の画像領域とを合成するステップとを有する認証情報を画像の一手段に隠し込む方法を提供する。

【００１４】第４の発明は，第１の画像領域と，データを操作することにより情報が隠し込まれた第２の画像領域とを画像中において特定するステップと，第１の画像

5

領域中のデータから第１の認証情報を生成するステップと，第２の画像領域から，第２の認証情報を抽出するステップと，第１の認証情報が第２の認証情報と一致する場合に，画像が改変されていないと判断するステップとを有する画像の同一性を認証方法を提供する。

【００１５】

【作用】このような構成では，（第２の）認証情報が第２の画像領域中に隠し込まれる。（第２の）認証情報は，画像の同一性を認証するための情報であり，第１の画像領域の内容によって異なる固有なものである。もし，第１の画像領域内のデータが改変された場合，改変されたデータに基づき生成される第１の認証情報は，第２の画像領域中に隠し込まている第２の認証情報とは異なる値となる。従って，第２の画像領域中に隠し込まれた第２の認証情報を抽出し，それを第１の画像領域から新たに生成した第１の認証情報と比較すれば，画像が改変されているか否かを検証することができる。

【００１６】

【発明の実施の形態】

［デジタル・カメラ］図２は，本実施例におけるデジタル・カメラの画像処理系のブロック図である。撮影された対象は，光学系２１を介して，ＣＣＤ２２により電気的なアナログ信号に変換される。この信号は，信号処理部２３，領域分割部２４，ハイディング部２５及び領域合成部２６を有する画像処理部２７により処理され，デジタル信号である画像データＤ’として出力され，メモリー・カード等の記憶部２８に保存される。この画像データＤ’は，ハイディング部２５により，画像データＤ中の所定の画像領域にハッシュ値が隠し込まれているため，画像データＤと完全に同一なデータではないが，視覚的にその相違を見分けることはできない。

【００１７】信号処理部２３の出力である画像データＤは，領域分割部２４により，２つの領域に切り分けられる。図３は，画像領域の分割及び合成を説明するための概念図である。同図（ａ）のような画像Ｄは，ハッシュ値生成のための入力値を与える画像領域D_1と生成されたハッシュ値Ｈを埋め込む画像領域D_2とに分割される（同図（ｂ）参照）。本実施例において，画像領域D_2は画像の右下の４０×４０画素で構成され，理想的には１６０ビットの情報を隠し込むことが可能である。

【００１８】領域分割部２３により分割された画像領域D_1は，認証情報生成部としてのダイジェスト計算部２９に入力される。ダイジェスト計算部２９は，切り取られた画像領域D_1全体のデータのハッシュ値Ｈを認証情報として計算する。ハッシュ値は，画像データに基づいた演算により画像の特徴を示すダイジェストである。ダイジェストとは，画像データの特徴を示す要約であり，ダイジェストとしてのハッシュ値Ｈは，画像内容の一画素の変更に対しても敏感に反応し，全く異なる値に変わるという性質を有する。従って，特に自然画像データとほぼ１対１の関係にある数値であると考えることができる。

6

【００１９】ハッシュ値Ｈは，具体的には以下の式で表現される。

【数１】

Ｈ＝Ｈ１（ｄ[0]//ｄ[1]//ｄ[2]//・・・//ｄ[I]）

【００２０】ここで、Ｈ１はハッシュ関数である。また、演算子「//」は、メッセージ配列の各要素をつなげるという意味である。また，ｄ[i]は，画像領域D_1中に含まれる各画素値を示している。この具体的な演算は、例えば、配列要素が有するデータの排他的論理和でもよい。但し、排他的論理和とした場合には、メッセージ配列値の順序は計算結果に反映されない。例えば、ＣＲＣ(Cyclic Redundancy Check)という方法を用いれば、この順序関係を反映することができる。このアルゴリズムは、、チェックサムを計算するためのアルゴリズムの一つで、データ列の内容及びデータ列の順序に依存した出力を生成する。

【００２１】このハッシュ関数Ｈ１は、バイト長がB_mバイトである入力（配列値ｄ[i]）に対して、それと異なるバイト長Ｋの出力（ハッシュ値）を求める関数である。この関数は一方向関数であるから、Ｈ(x)＝yにおいて、yからxを推定することは、事実上不可能である。ハッシュ値は、データ・ハイディングの際に単に初期値として用いられるものであり、異なる入力に対して異なる出力が事実上保証されていれさえすればよい。従って、ハッシュ値の値自身には特別な意味はない。重要なことは、その演算により配列の特徴を示す値を出力すること、つまり配列要素全体の内容に基づいてハッシュ値が一意に定まり、かつその値が配列全体の内容により異なることである。

【００２２】暗号変換部３０は，ハッシュ値Ｈを秘密鍵ＳＫを用いて暗号化し，暗号化されたハッシュ値Ｈ’を出力する。この暗号化されたハッシュ値Ｈ’が認証情報である。秘密鍵ＳＫは，デジタル・カメラごとに異なる鍵を用いるものとし，カメラ内部に保持されている

【００２３】認証情報として暗号化されたハッシュ値Ｈ’は，画像処理部２７中のハイディング部２５に送られる。ハイディング部２５は，画像領域中D_2のデータを操作することにより，ハッシュ値Ｈ’を画像領域D_2中に隠し込む。隠し込みは，実空間又は周波数空間において，画像領域D_2中のデータ（例えば画素値）を操作することにより行うことが可能である。埋め込みは様々な方法が考えられるが，その具体例については後述する。なお，これに関しては，特願平８－１５９３３０号（当方整理番号ＪＡ９９６－０４４）及び特願平８－２７２７２１号（当方整理番号ＪＡ９９６－０７４）にも詳細に説明されている。

【００２４】画像領域D_2中には，ハッシュ値Ｈ’を隠し込むため，その領域内のデータを操作しているので，

その部分における画質は，原画像と多少相違している。しかしながら，視覚的にはこのような相違を認識することはほとんど不可能なので，画質の視覚的な劣化は生じない。

【００２５】領域合成部２６は，原画像中の画像領域Ｄ1とハッシュ値Ｈ’が隠し込まれた画像領域D_2とを合成する（図３（ｃ）参照）。そして，この合成された画像データＤ’を記憶部２８中に保存する。

【００２６】上記の説明から明らかなように，画像領域の分割は，ダイジェストの計算とは関係しない埋め込む領域を特定するために行われる。もし，画像領域を分割せずに，画像全体のダイジェストを計算して，その結果を隠し込んだとすると，この隠し込み後の画像全体の新たなダイジェストは，埋め込まれている元のダイジェストと一致しなくなる。従って，このような方法では，画像の同一性の認証を行うことができない。そこで，ダイジェストを隠し込む画像領域は，ダイジェスト計算の対象としないことにより，計算されたダイジェストと隠し込まれているダイジェストとの一致を保証しているのである。このような観点において，画像領域D_2の部分だけを黒や白等の単色で塗りつぶした原画像Ｄを画像領域D_1としてもよい。この場合，一部が塗りつぶされた原画像Ｄのダイジェストを計算して，それを画像領域D_2に隠し込む。これにより，隠し込み後においてもダイジェストの一致を保証することができる。

【００２７】なお，本実施例におけるデジタル・カメラは，撮影カメラのＩＤ，撮影の日付等のタイム・スタンプ，ＧＰＳで測定される位置情報といった付加情報を画像領域D_1中に隠し込んでおいてもよい。この場合には，まず，画像領域D_1中に付加情報を隠し込んんで，その後に，その結果のハッシュ値Ｈ’を画像領域D_2に隠し込むことが重要である。なぜなら，付加情報を埋め込む前の画像のハッシュ値Ｈ’を画像領域D_2に隠し込むと，その後の付加情報の隠し込みにより，ハッシュ値が相違してしまうため，同一性の認証ができなくなるからである。

【００２８】なお，画像領域D_2は，上記の実施例のように一箇所に集中している必要はなく，位置系列生成アルゴリズムを用いて分散して存在させてもよいし，Low Bitの一部だけ用いてもよい。

【００２９】［画像認証システム］次に，隠し込まれた認証情報を用いて，デジタル・カメラで撮影された画像の同一性認証を行うシステムについて説明する。同一性を検証しようとする者は，以下の情報を有している必要がある。認証情報は，画像中に一体不可分な状態で隠し込まれているため，別ファイルの形式で保管している必要はない点に留意されたい。

（１）画像データＭ’

（２）秘密鍵ＳＫに対応した公開鍵ＰＫ（権限を有する者から別途入手）

【００３０】図４は，本実施例における画像の同一性認証システムのブロック図である。領域特定部４１は，ハッシュ値Ｈ’が隠し込まれている画像Ｄ’において，画像領域D_1と画像領域D_2とを特定する。画像領域Ｄ1は，ハッシュ値を生成するためのデータを与える領域であり，画像領域D_2は，上述の認証情報としてのハッシュ値Ｈ’が隠し込まれている領域である。

【００３１】ダイジェスト計算部４２は，画像領域D_1中のデータに基づいて，ハッシュ値を新たに計算する。また，ダイジェスト抽出部４３は，画像領域D_2から，認証情報として隠し込まれている暗号化されたハッシュ値Ｈ’を抽出する。具体的な抽出方法は，具体的な埋め込む方法と共に後述する。

【００３２】復号変換部４４は，抽出されたハッシュ値Ｈ’を，公開鍵ＰＫを用いて復号する。この公開鍵ＰＫは，秘密鍵ＳＫに対応して一意に定まる入手可能な鍵であり，これを保管している権限ある者から入手する必要がある。

【００３３】認証部４５では，ダイジェスト計算部４２により新たに計算された画像領域D_1中のデータに基づいたハッシュ値と，復号変換部４４により得られたハッシュ値Ｈ’とを比較することにより同一性の認証を行う。すなわち，ハッシュ値が一致する場合は，画像が改ざんされていないと判断する。また，ハッシュ値が一致しない場合は，画像が改ざんされていると判断する。ハッシュ値が一致しないケースが生じるのは以下の２つの少なくとも一方に該当する場合である。

（１）画像領域D_1が改ざんされている場合
画像領域D_1から新たに再測したハッシュ値が変わるので，画像領域D_2中に隠し込まれたハッシュ値Ｈと一致しなくなる。

（２）画像領域D_2が改ざんされている場合
画像領域D_2に隠し込まれたハッシュ値Ｈが変わるので，画像領域D_1から再測したハッシュ値と一致しなくなる。

【００３４】本実施例によれば，データ・ハイディング技術を用いることにより，認証情報が画像中に一体化して隠し込まれているため，認証情報を画像データに別ファイルとして添付する必要がない。従って，検証者が認証情報を特に保持していなくとも検証を実施することができる。

【００３５】また，公開鍵暗号方式を用いて，認証情報を暗号化（スクランブル）しているので，悪意の第三者による認証情報の書き換えを事実上不可能にすることができる。さらに，ある公開鍵ＰＫは，ただ１つの秘密鍵ＳＫに対応している。従って，秘密鍵ＳＫは，デジタル・カメラごとに相違させることにより，そのデジタル画像がどのデジタル・カメラで撮影されたのかを認証することも可能である。

【００３６】なお，デジタル・カメラを開封して本体内

部の保持情報への不正なアクセスに対抗するために，携帯電話等で用いられている耐タンパー・モジュールなどのデバイスを利用することが有効である。このような不正アクセスが行われた場合，秘密鍵ＳＫが盗難されたものとみなして，その秘密鍵ＳＫによる画像データについては，ダイジェストが一致した場合でも，改ざんされたもの判定する。このようにすることで，第三者の不正な行為による被害を避けることができる。

【００３７】なお，上記実施例は，デジタル・カメラについて説明したが，本発明はこれに限定されるものではなく，デジタル・ビデオなどのデジタル・システムに広く利用できることは当然である。

【００３８】

【実施例】ここでは、隠ぺいの対象となるデータをあるあるメディア・データ中に埋め込む方法及び逆に埋め込まれたデータを抽出する方法の一例であるピクセル・ブロック・コーディング(Pixel Block Coding)（以下、ＰＢＣという）について説明する。ＰＢＣを用いた場合、データをハイディング及び抽出は、以下の述べるようなある変換規則に従って処理される。

【００３９】［基本アルゴリズム］一般的に、隣接した２つの画素の画素値等の１次特性は互いに高い相関関係を有している。従って、画素値を入れ変えたとしても、画像が視覚的に認識できる程度の劣化は生じない。この性質に鑑みて、本アルゴリズムは、少なくとも１つの画素を有する画像領域をピクセル・ブロックとして定義し、ある変換規則に基づき意図的に隣接したピクセル・ブロックの特性値を入れ替えることで、１ビットのデータを隠ぺいする。すなわち、データは、隣接するピクセル・ブロックの特性値の入れ替えにより表現される。また、データの抽出時には、この変換規則に基づき決定される抽出規則に従って、データを抽出する。

【００４０】ビット情報は、隣接した２つのピクセル・ブロックの特性値（例えば、輝度値）を以下の変換規則に従って入れ替えること表現される。

【００４１】ビット・オン〈1〉:　一方のピクセル・ブロック（PB_1）の特性値が他方（PB_2）の特性値より大きい場合

ビット・オフ〈0〉:　一方のピクセル・ブロック（PB_1）の特性値が他方（PB_2）の特性値より小さい場合

【００４２】また、ビット情報は、以下の抽出規則に従って、隣接した２つのピクセル・ブロックの特性値（例えば、輝度値）を比較することにより抽出される。

【００４３】一方のピクセル・ブロック（PB_1）の特性値が他方（PB_2）の特性値より大きい場合：ビット・オン〈1〉

一方のピクセル・ブロック（PB_1）の特性値が他方（PB_2）の特性値より小さい場合：ビット・オフ〈0〉

【００４４】図５は、ＰＢＣを用いたデータのハイディング及び抽出を説明するための図である。ピクセル・ブロックPB_1、PB_2は例えば３×３画素のように複数の画素の集合として定義してもよいし、１画素を１ピクセル・ブロックと定義することも可能である。隣接するピクセル・ブロックは高い相関を有しているので、それらの位置を入れ替えたとしても、画像が視覚的に認識できる程度に劣化したとは感じることはないであろう（図５（ａ））。

【００４５】オリジナル画像におけるピクセル・ブロックの位置が同図（ｂ）である場合を考える。まず、二つのピクセル・ブロックの特性値を比較し、その結果、PB_1の特性値の方がPB_2の特性値よりも大きいとする。オリジナルにデータ”１”を隠ぺいする場合、ピクセル・ブロックの特性値が、変換規則におけるデータ”１”の条件を既に満たしているので、これらのブロックの特性値の入れ替え行われない。データを抽出する際、ＰＢ1の特性値が大きい場合はデータ”１”であると抽出規則が定めているので、データ”１”が抽出される。

【００４６】一方、オリジナルにデータ”０”を隠ぺいする場合、オリジナルにおけるピクセル・ブロックの特性値の関係が、変換規則におけるデータ”０”の条件を満たさないので、ピクセル・ブロックの特性値を入れ替える。しかしながら、この入れ替えは視覚的には認識できない。抽出時は、抽出規則に従って、これらのブロックの特性値の関係からデータ”０”が抽出される。

【００４７】このようにＰＢＣでは、隠ぺいの対象となる情報を隠ぺいするのに十分な数のピクセル・ブロックを画像中から選択する。そして選択された一のピクセル・ブロックとそれに隣接するピクセル・ブロックのペアを作ることにより、このペアの列を生成する。そして、列の先頭から順々に隠ぺい対象となるビットを隠ぺいしていく。

【００４８】この列は、第１の実施例における状態系列Ｓに対応付けてもよい。例えば、ピクセル・ブロックを第１の実施例におけるメディア配列Ｍの配列要素Ｍに対応付ける。ハイディング作業において逐次的に生成された状態系列の各配列要素（状態値S_j）及びそれに隣接するメディア配列値とでペアを作る。そして、このペアに対して上記処理を施すことが考えられるまた、ある乱数の種（シード）から発生される疑似乱数列をもとに決定することももちろん可能である。

【００４９】抽出時には、ハイディング時と同じブロック列をスキャンする。それぞれのペアがビット・オンを表すかオフを表すかを抽出規則に従って１ビットずつ集めることで全体のメッセージを抽出する。もし、ペアであるピクセル・ブロックの特性値が同じであるならば、そのペアはハイディング時と同様にスキップする。ブロック列あるいはその列生成方法を秘密にすれば、隠ぺいされた情報を他人から隠すことができる。

【００５０】なお，ＰＢＣにおいて，埋め込み位置は，画質及び抽出精度に鑑みて決定するのが好ましい。すな

わち，埋め込み対象となっているペアを構成するピクセル・ブロックの特性値の差があまり大きいと，入れ替え操作により画質が劣化するおそれがある。このような画質の劣化を抑制するために，第１の閾値（上限）を設けておき，特性値の差がその閾値以上であれば，そのペアにはビットを埋め込まないようにすることが好ましい。

【００５１】また，特性値の差が小さければ，入れ替え操作による画質の劣化はほとんど生じないが，逆にノイズの影響により大小関係が反転してしまい，抽出時に埋め込まれたビットが抽出できないおそれがある。従って，抽出精度の低下を抑制するためには，第２の閾値（下限）を設けておき，特性値の差がその閾値以下であれば，そのペアにはビットを埋め込まないようにすることが好ましい。

【００５２】これらのケースに該当するペアには何も操作を施すことなくスキップする。そして、隠ぺいすべきビット情報を先送りして、次のペアを対象に隠ぺいする。

【００５３】［ブロックの特性値］特性値として、ピクセル・ブロックの１次特性に関する値及び２次特性に関する値を用いることできる。１次特性は、ピクセル・ブロックの輝度や色度のように画素値の直接的なパラメータである。また、２次特性は、前記パラメータの平均値や分散といった統計的な性質を示す値のように、１次特性をを分解することで得られる。さらに，特性値は，複数の画素値からなる配列と所定の配列（マスク）との演算結果としてもよく，周波数変換を行うことにより得られる特定の要素値とすることも可能である。一般に、１次特性は隣接する２つのピクセル・ブロックにおいて高い相関関係を有している。これに対して、２次特性は隣接しない離れた二つのブロックにおいて高い相関関係を有し得る。従って、ｐＢＣの対象となるピクセル・ブロックは、必ずしも隣接するブロックに限定されない点に留意されたい。

【００５４】

【効果】このように本発明によれば，認証情報は画像データと一体不可分な形式，すなわち画像中に隠し込まれた形式で供給されるので，検証者は認証情報を別に保管しておく必要がない。このような認証情報の隠し込みを行っても画像データの画質を劣化させることはない。

【図面の簡単な説明】

【図１】従来のデジタル・カメラの画像処理系のブロック図である。

【図２】本実施例におけるデジタル・カメラの画像処理系のブロック図である。

【図３】本実施例における画像の同一性認証システムのブロック図である。

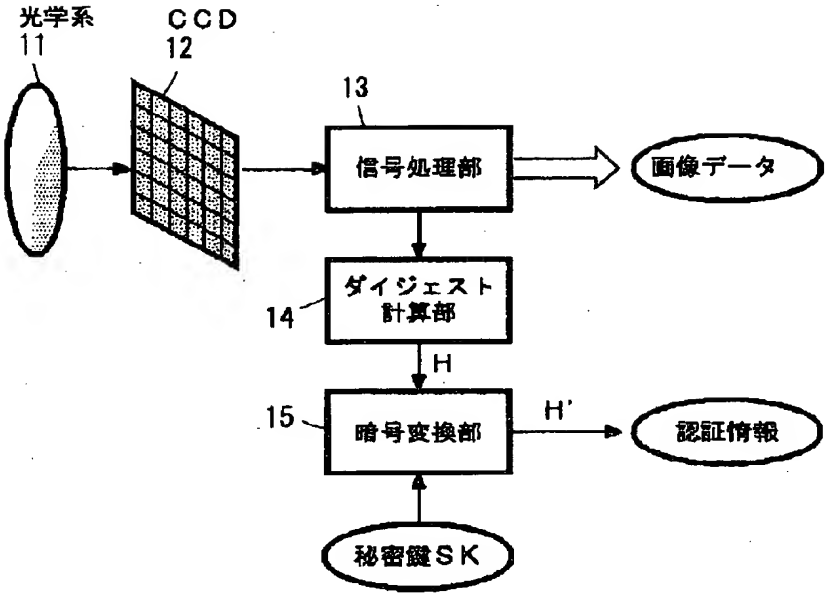
【図４】本実施例における画像の同一性認証システムのブロック図である。

【図５】ＰＢＣを用いたデータのハイディング及び抽出を説明するための図である。

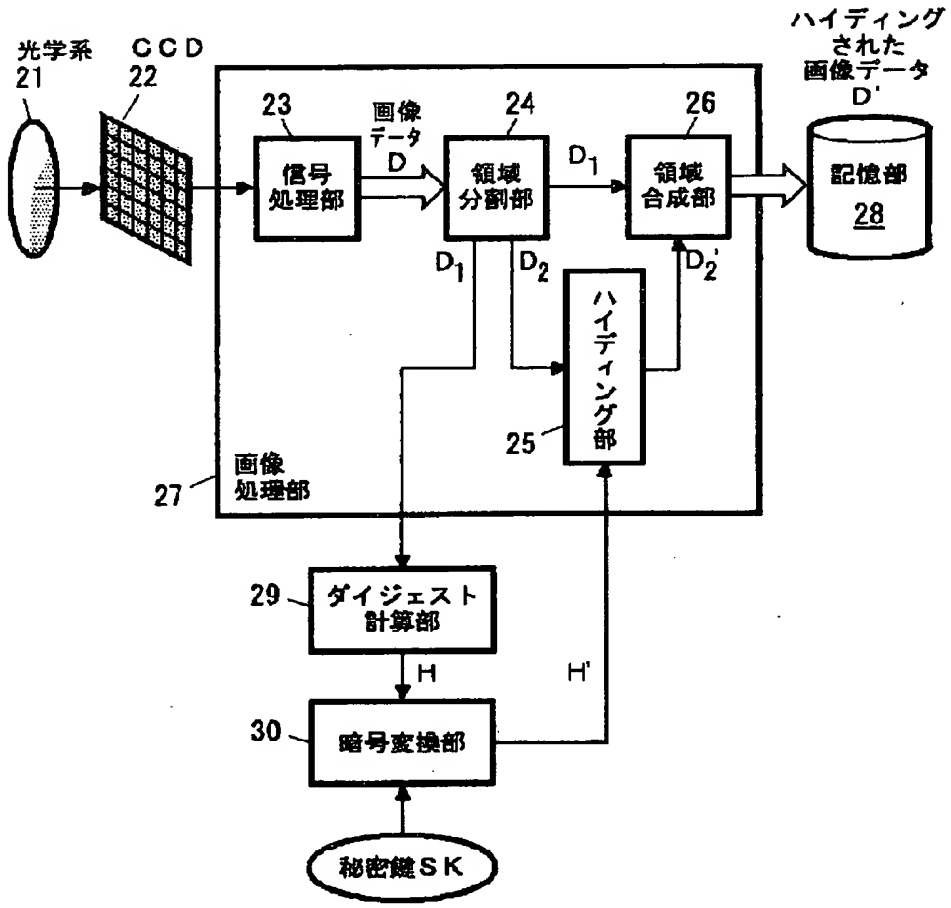
【符号の説明】

２１・・・光学系
２２・・・ＣＣＤ
２３・・・信号処理部
２４・・・領域分割部
２５・・・ハイディング部
２６・・・領域合成部
２７・・・画像処理部
２８・・・記憶部
２９・・・ダイジェスト計算部
３０・・・暗号変換部

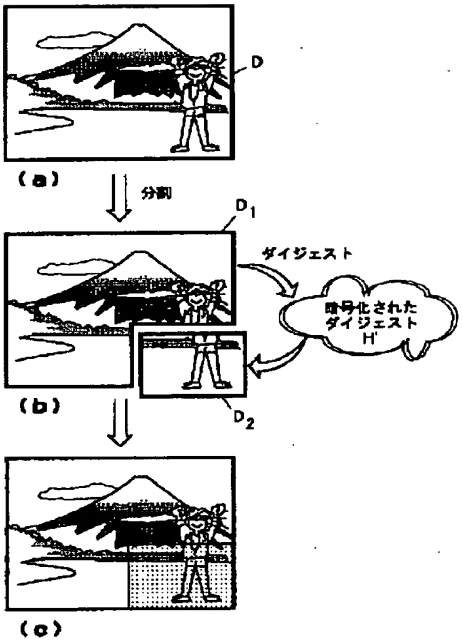
【図１】


光学系
11
CCD
12
13
信号処理部
画像データ
ダイジェスト
計算部
14
H
15
暗号変換部
H'
認証情報
秘密鍵ＳＫ

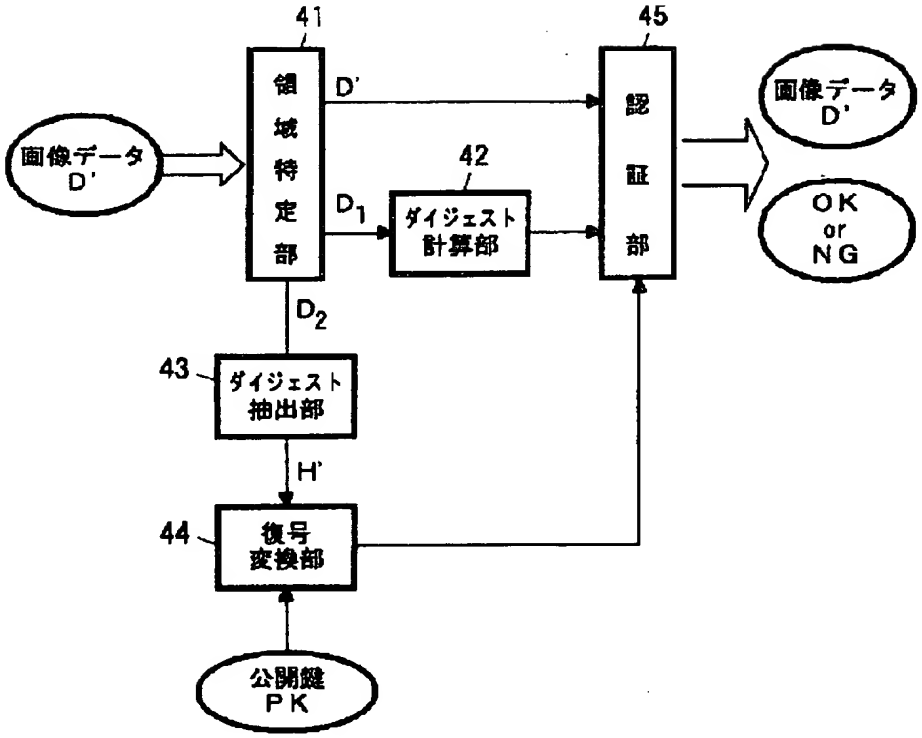
【図２】


光学系
21
CCD
22
23
信号
処理部
画像
データ
D
24
領域
分割部
D1
26
領域
合成部
ハイディング
された
画像データ
D'
記憶部
28
D1
D2
D2'
ハイディング
部
25
画像
処理部
27
29
ダイジェスト
計算部
H
H'
30
暗号変換部
秘密鍵ＳＫ

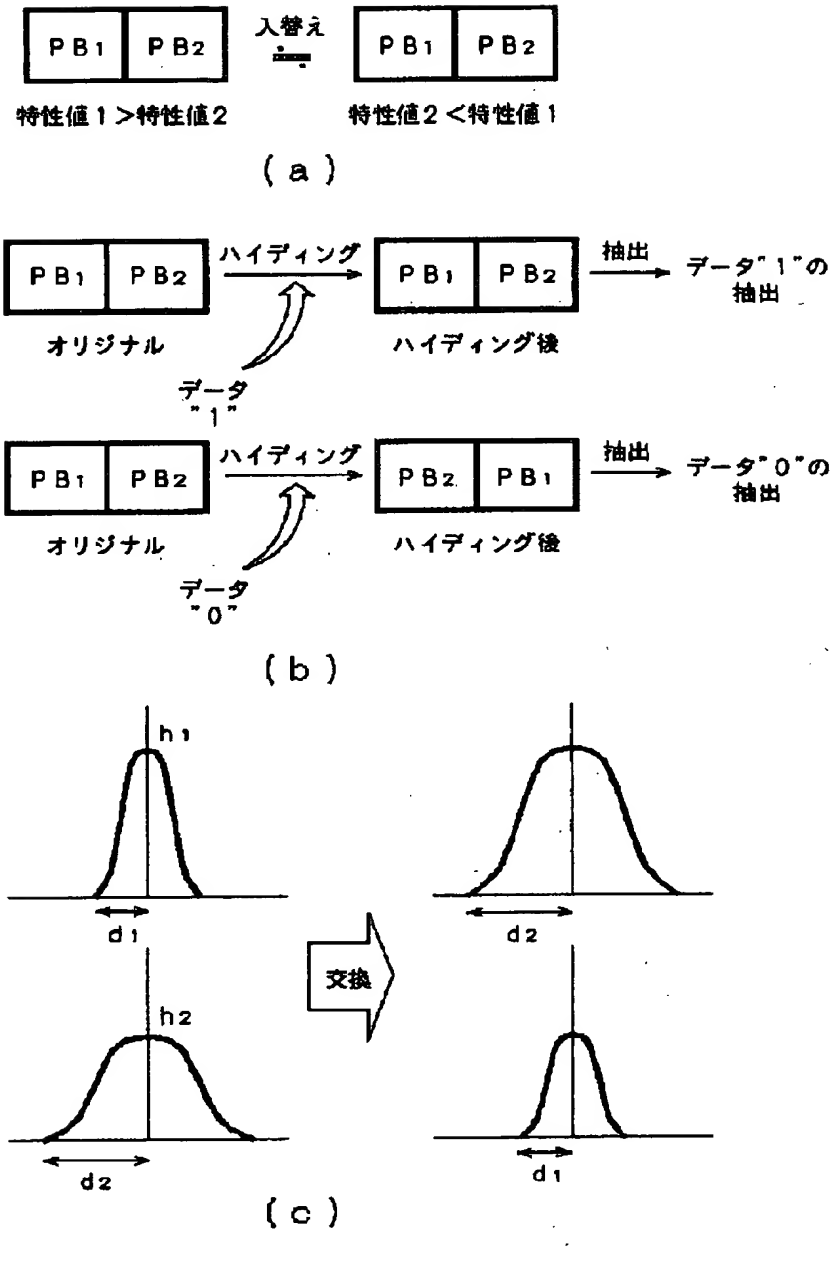
【図３】


D
(a)
分割
D1
ダイジェスト
暗号化された
ダイジェスト
H'
(b)
D2
(c)

【図４】


41
領域特定部
45
認証部
画像データ
D'
D'
画像データ
D'
42
D1
ダイジェスト
計算部
OK
or
NG
D2
43
ダイジェスト
抽出部
H'
44
復号
変換部
公開鍵
PK

【図５】


PB1
PB2
入替え
特性値１>特性値２
特性値２<特性値１
(a)
ハイディング
抽出
データ"１"の抽出
オリジナル
ハイディング後
データ"１"
データ"０"の抽出
データ"０"
(b)
h1
d1
d2
交換
h2
(c)